What is claimed is:

1. A method of returning change to a payer in an electronic payment system wherein a due amount is paid by a payer to a payee via a first payment certificate having a value of a first amount higher than a due amount, the method comprising:

receiving, by a payment provider, of the first payment certificate;

verifying, by the payment provider, of the first payment certificate;

crediting, by the payment provider, of the due amount to the payee;

determining, by the payer, of at least one change return value such that the sum of the determined at least one change return value is equal to a difference between the first amount and the due amount;

generating, by the payer, of at least one change return certificate according to the at least one change return value;

blinding, by the payer, of the change return certificate;

generating, by the payer, of a first signature by signing the blinded change return certificate;

sending, by the payer, of a message comprising the first signature to the payee;

forwarding, by the payer, of the message to the payment provider;

verifying, by the payment provider, of the first signature;

verifying, by the payment provider, of a change return value indicated by the message;

generating, by the payment provider, of a blinded second signature by signing the blinded change return certificate if the verification of the first signature and of the change return value is successful;

forwarding, by the payment provider, of the blinded second signature to the payer;

unblinding, by the payer, of the blinded second signature;

verifying, by the payer, of the second signature;

forming, by the payer, of at least one second payment certificate by linking the change return certificate and the unblinded second signature.

2. The method of claim 1, further comprising:

assigning, by the payment provider, of a second asymmetric key pair comprising a second public key and a second private key to a change return value;

blinding, by the payer, of the change return certificate via a blinding factor, the blinding factor being encrypted via the second public key;

generating, by the payment provider, of the blinded second signature by signing the blinded change return certificate via the second secret key;

wherein the step of unblinding of the blinded second signature by the payer comprises a division of the blinded second signature by the blinding factor;

wherein the step of verifying the second signature by the payer comprises a decryption of the unblinded second signature and a test of whether the decrypted unblinded second signature corresponds to a generated change return certificate.

3. The method of claim 1, wherein the payment provider sends the second public key to the payee and the payee forwards the second public key to the payer.

4. A method of performing tasks of a payment provider in a change returning transaction in an electronic payment system, wherein a payment provider receives a first payment certificate having a value of a first amount higher than the due amount and verifies the first payment certificate and credits the due amount to a payee, the method comprising:

receiving a message comprising a first signature of a blinded change return certificate;

verifying the first signature;

verifying a change return value indicated by the message;

generating a blinded second signature by signing the blinded change return certificate if the verification of the first signature and of the change return value is successful; and

sending the second signature to the payee.

5. The method of claim 4, wherein:

a second asymmetric key pair comprising a second public key and a second private key is assigned by the payment provider to the change return value;

the change return certificate is blinded by means of a blinding factor encrypted via the second public key; and

the blinded second signature is generated by the payment provider by signing the blinded change return certificate by means of the second secret key.

6. The method of claim 4, wherein the message comprising the first signature includes the first payment certificate in order to perform crediting of the first amount.

7. The method of claim 4, wherein:

a first asymmetric key pair comprising a first public key and a first private key is assigned to the first payment certificate;

the first payment certificate comprises the first public key;

the first signature is generated by the payer via the first private key; and

the verification of the first signature is performed by the payment provider via the first public key.

8. The method of claim 4, wherein:

the first signature indicates the value of the first amount of the first payment certificate; and

the payment provider verifies the value of the first amount of the first payment certificate.

9. The method of claim 4, wherein the payment provider stores at least one of the first signature and the message comprising the first signature.

10. A method of performing tasks of a payer in a change returning transaction in an electronic payment system wherein the payer pays a due amount by means of a first payment certificate having a value of a first amount higher than the due amount, the method comprising:

determining at least one change return value such that the sum of the determined change return values is equal to a difference of the first amount and the due amount;

generating at least one change return certificate according to the at least one change return value;

blinding the change return certificate;

generating a first signature by signing the blinded change return certificate;

sending a message comprising the first signature to a payee;

receiving a blinded second signature comprising a signed blinded change return certificate;

unblinding the blinded second signature;

verifying the second signature; and

forming at least one second payment certificate by linking the change return certificate and the unblinded second signature.

11. The method of claim 10, wherein:

a first asymmetric key pair comprising a first public key and a first private key is assigned to the first payment certificate;

the first payment certificate comprises the first public key;

the first signature is generated by means of the first private key.

12. The method of claim 10, wherein

a second asymmetric key pair comprising a second public key and a second private

key is assigned to a change return value;

the change return certificate is blinded by means of a blinding factor encrypted by means of the second public key;

the unblinding of the blinded second signature comprises a division of the second signature by the blinding factor;

the verification of the second signature comprises the decryption of the unblinded second signature and a test of whether the decrypted unblinded second signature corresponds to a generated change return certificate.

13. The method of claim 10, wherein the first signature indicates the value of the first amount of the first payment certificate.

14. The method of claim 10, further comprising receiving the second public key.

15. The method of claim 10, wherein at least one of the second payment certificate and a private key corresponding to the second payment certificate is sent to a third party for storing as a backup.

16. The method of claim 10, wherein the first signature is generated by signing the blinded change return certificate and a change return value linked to the blinded change return certificate.

17. The method of claim 10, wherein the message comprises at least one of the blinded change return certificate and the change return value corresponding to the blinded change return certificate.

18. The method of claim 10, wherein the first payment certificate comprises a macropayment certificate.

19. The method of claim 10, wherein the first payment certificate comprises a micropayment certificate.

20. The method of claim 10, wherein the blinding of the change return certificate comprises building a digest of the change return certificate and blinding the digest.

21. The method of claim 10, wherein the message comprising the first signature includes the first payment certificate in order to perform the payment of the first amount.

22. An article of manufacture for returning change to a payer in an electronic payment system, wherein a due amount is paid by a payer to a payee via a first payment certificate having a value of a first amount higher than a due amount, the article of manufacture comprising:

at least one computer readable medium;

processor instructions contained on the at least one computer readable medium, the processor instructions configured to be readable from the at least one computer readable medium by at least one processor and thereby cause the at least one processor to operate as to:

receive the first payment certificate;

verify the first payment certificate; and

credit the due amount to the payee;

wherein the payer determines at least one change return value such that the sum of the determined at least one change return value is equal to a difference between the first amount and the due amount;

wherein the payer generates at least one change return certificate according to the at least one change return value;

wherein the payer blinds the change return certificate,

wherein the payer generates a first signature by signing the blinded change return certificate;

wherein the payer sends a message comprising the first signature to the payee;

wherein the payer forwards the message to the payment provider;

the processor instructions being further configured to be readable from the at least one computer readable medium by the at least one processor and thereby cause the at least one processor to operate as to:

verify the first signature;

verify a change return value indicated by the message;

generate a blinded second signature by signing the blinded change return certificate if the verification of the first signature and of the change return value is successful; and

forward the blinded second signature to the payer;

wherein the payer unblinds the blinded second signature;

wherein the payer verifies the second signature; and

wherein the payer forms at least one second payment certificate by linking the change return certificate and the unblinded second signature.

23. A payment device comprising:

means for determining at least one change return value such that the sum of the determined at least one change return value is equal to a difference of a first amount and a due amount;

means for generating at least one change return certificate according to the at least one change return value;

means for blinding the change return certificate;

means for generating a first signature by signing the blinded change return certificate;

means for sending a message comprising the first signature to a payee;

means for unblinding a blinded second signature comprising a signed blinded change return certificate;

means for verifying the second signature; and

means for forming at least one second payment certificate by linking the change return certificate and the unblinded second signature.

24. The payment device of claim 23, wherein the payment device comprises a mobile phone.

25. A bank device adapted to perform tasks of a payment provider in a change returning transaction in an electronic payment system, the bank device comprising:

means for receiving a message comprising a first signature of a blinded change return certificate;

means for verifying the first signature;

means for verifying a change return value indicated by the message;

means for generating a blinded second signature by signing the blinded change return certificate if the verification of the first signature and of the change return value is successful; and

means for sending the second signature to the payee.